AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1. (Currently amended) A method for facilitating secure communication

2 between two networked devices, comprising:

3   establishing communication between a situation notification device and a

4 provisioning device over a preferred channel, wherein the preferred channel is

5 bidirectional, location-limited, has a demonstrative identification property and an

6 authenticity property, and does not require being resistant to eavesdropping;

7   wherein the demonstrative identification property allows a human

8   operator to be aware of which devices are communicating with each other

9   based on physical proximity; and

10   wherein the authenticity property makes it difficult or impossible

11   for attacking devices to tamper with or alter messages transmitted in the

12   preferred channel, or to insert false information into the preferred channel

13   without being detected by legitimate participants communicating via the

14   preferred channel;

15   prior to establishing the communication, pre-authenticating the situation

16 notification device to ensure that the situation notification device has physical

17 access to the preferred channel, wherein pre-authenticating the situation

18 notification device involves:

19   exchanging key commitment information between the provisioning

20   device and the situation notification device over the bidirectional preferred

21   channel;

22   exchanging keys between the provisioning device and the situation

23   notification device over a bidirectional channel which does not have to be

24   the preferred channel; and

25   verifying the received keys using the received key commitment

26   information on both the provisioning device and the situation notification

27   device;

28   providing provisioning information to said situation notification device

29 over said preferred channel, wherein said situation notification device is

30 automatically configured to receive subject matter information responsive to said

31 provisioning information;

32   receiving said subject matter information;

33   verifying said subject matter information with said provisioning

34 information; and

35   presenting said subject matter information to a user of the situation

36 notification device responsive to the step of verifying, wherein the step of

37 verifying ensures that the subject matter information is genuine.

1   2. (Previously presented) The method of claim 1, wherein the step of

2 providing further comprises:

3   exchanging key commitment information over said preferred channel

4 between said provisioning device and said situation notification device;

5   receiving a public key by said situation notification device;

6   verifying said public key with said key commitment information; and

7   receiving a credential authorized by a credential issuing authority.

1   3. (Previously presented) The method of claim 1, wherein said preferred

2 channel is a location-limited channel.

1   4. (Previously presented) The method of claim 1, wherein said preferred

2   channel uses a telephone switching system.

1   5. (Canceled)

1   6. (Previously presented) The method of claim 1, wherein subject matter

2   information is received using an antenna, a telephone line, a local area network, a

3   wide area network, a wireless network, or a broadcast network.

1   7. (Previously presented) The method of claim 1, wherein said situation

2   notification device is a computer, a television, a radio, a telephone, a push to talk

3   device, a pager, a clock, a thermostat, a network appliance, or a home appliance.

1   8. (Previously presented) The method of claim 1, further comprising

2   forwarding said subject matter information.

1   9. (Previously presented) The method of claim 1, wherein said subject

2   matter information is alarm information.

1   10. (Currently amended) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to present

3   subject matter information, the method comprising steps of:

4   establishing communication between a situation notification device and a

5   provisioning device over a preferred channel, wherein the preferred channel is

6   bidirectional, location-limited, has a demonstrative identification property and an

7   authenticity property, and does not require being resistant to eavesdropping;

4

8	wherein the demonstrative identification property allows a human
9	operator to be aware of which devices are communicating with each other
10	based on physical proximity; and
11	wherein the authenticity property makes it difficult or impossible
12	for attacking devices to tamper with or alter messages transmitted in the
13	preferred channel, or to insert false information into the preferred channel
14	without being detected by legitimate participants communicating via the
15	preferred channel;
16	prior to establishing the communication, pre-authenticating the situation
17	notification device to ensure that the situation notification device has physical
18	access to the preferred channel, wherein pre-authenticating the situation
19	notification device involves:
20	exchanging key commitment information between the provisioning
21	device and the situation notification device over the bidirectional preferred
22	channel;
23	exchanging keys between the provisioning device and the situation
24	notification device over a bidirectional channel which does not have to be
25	the preferred channel; and
26	verifying the received keys using the received key commitment
27	information on both the provisioning device and the situation notification
28	device;
29	providing provisioning information to said situation notification device
30	over said preferred channel, wherein said situation notification device is
31	automatically configured to receive said subject matter information responsive to
32	said provisioning information;
33	receiving said subject matter information;
34	verifying said subject matter information with said provisioning
35	information; and

5

36   presenting said subject matter information to a user of the situation

37   notification device responsive to the step of verifying, wherein the step of

38   verifying ensures that the subject matter information is genuine.

1   11. (Original) The computer-readable storage medium of claim 10,

2   wherein the step of providing

3   further comprises:

4   exchanging key commitment information over said preferred channel

5   between said provisioning device and said situation notification device;

6   receiving a public key by said situation notification device;

7   verifying said public key with said key commitment information; and

8   receiving a credential authorized by a credential issuing authority.

1   12. (Original) The computer-readable storage medium of claim 10,

2   wherein said preferred channel is a location-limited channel.

1   13. (Original) The computer-readable storage medium of claim 10,

2   wherein said preferred channel uses a telephone switching system.

1   14. (Canceled)

1   15. (Original) The computer-readable storage medium of claim 10,

2   wherein subject matter information is received using an antenna, a telephone line,

3   a local area network, a wide area network, a wireless network, or a broadcast

4   network.

1   16. (Original) The computer-readable storage medium of claim 10,

2   wherein said situation notification device is a computer, a television, a radio, a

3   telephone, a push to talk device, a pager, a clock, a thermostat, a network

4   appliance, or a home appliance.

1   17. (Original) The computer-readable storage medium of claim 10, further

2   comprising forwarding said subject matter information.

1   18. (Original) The computer-readable storage medium of claim 10,

2   wherein said subject matter information is alarm information.

1   19. (Currently amended) An apparatus comprising:

2   at least one port configured to establish a preferred channel, wherein the

3   preferred channel is bidirectional, location-limited, has a demonstrative

4   identification property and an authenticity property, and does not require being

5   resistant to eavesdropping;

6   wherein the demonstrative identification property allows a human

7   operator to be aware of which devices are communicating with each other

8   based on physical proximity; and

9   wherein the authenticity property makes it difficult or impossible

10   for attacking devices to tamper with or alter messages transmitted in the

11   preferred channel, or to insert false information into the preferred channel

12   without being detected by legitimate participants communicating via the

13   preferred channel;

14   a first communication mechanism configured to receive provisioning

15   information over said preferred channel, whereby the apparatus is configured to be

16   able to receive subject matter information responsive to said provisioning

17   information,

18   wherein the port is further configured to pre-authenticate the first

19   communication mechanism prior to receiving the provisioning information to

20   ensure that the first communication mechanism has physical access to the

21   preferred channel, wherein pre-authenticating the situation notification device

22   involves:

23   exchanging key commitment information between the provisioning

24   device and the situation notification device over the bidirectional preferred

25   channel;

26   exchanging keys between the provisioning device and the situation

27   notification device over a bidirectional channel which does not have to be

28   the preferred channel; and

29   verifying the received keys using the received key commitment

30   information on both the provisioning device and the situation notification

31   device;

32   a second communication mechanism configured to receive said subject

33   matter information subsequent to operation of the first communication

34   mechanism;

35   a verification mechanism configured to verify said subject matter

36   information with said provisioning information; and

37   a presentation mechanism configured to present said subject matter

38   information to a user of the situation notification device responsive to the

39   verification mechanism, wherein the step of verifying ensures that the subject

40   matter information is genuine.

1   20. (Original) The apparatus of claim 19, wherein the first communication

2   mechanism further comprises:

3   a key commitment receiver mechanism configured to receive key

4   commitment information through said at least

5   one port;

6   a key receiver mechanism configured to receive a public key;

7   a pre-authentication mechanism configured to verify said public key with

8 said key commitment information; and

9   a credential provisioning mechanism configured to be able to

10 automatically provide a credential authorized by a credential issuing authority

11 responsive to the pre-authentication mechanism.

1   21. (Original) The apparatus of claim 19, wherein said preferred channel is

2 a location-limited channel.

1   22. (Original) The apparatus of claim 19, wherein said preferred channel

2 uses a telephone switching system.

1   23. (Canceled)

1   24. (Original) The apparatus of claim 19, wherein subject matter

2 information is received using an antenna, a telephone line, a local area network, a

3 wide area network, a wireless network, or a broadcast network.

1   25. (Original) The apparatus of claim 19, wherein the apparatus is within a

2 computer, a television, a radio, a telephone, a push to talk device, a pager, a clock,

3 a thermostat, a network appliance, or a home appliance.

1   26. (Original) The apparatus of claim 19, further comprising a forwarding

2 mechanism configured to forward said subject matter information.

1   27. (Original) The apparatus of claim 19, wherein said subject matter

2 information is alarm information.

1   28. (Previously Presented) The method of claim 1, wherein said preferred

2 channel has a demonstrative identification property and an authenticity property

1   29. (Previously Presented) The computer-readable storage medium of

2 claim 10, wherein said preferred channel has a demonstrative identification

3 property and an authenticity property.

1   30. (Previously Presented) The apparatus of claim 19, wherein said

2 preferred channel has a demonstrative identification property and an authenticity

3 property.